U.S. AND ALLIED CYBER SECURITY COOPERATION IN THE INDO-PACIFIC

Annotated Bibliography

March 30, 31 and April 1, 2021

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Annotated Bibliography

U.S. AND ALLIED CYBER SECURITY COOPERATION IN THE INDO-PACIFIC

Center for Global Security Research
Livermore, California, March 30, 31 and April 1, 2021

Prepared By: Brandon Williams, Jessica Budlong, Matthew O'Hare, Amanda Tobey, Emilyn Tuomala

Key Questions:

- How urgent is the regional cyber threat to the United States and its allies in the Indo-Pacific? What are its main characteristics? How might it evolve over the coming decade?
- What lessons can be drawn from past and present efforts to strengthen cooperation to address this threat?
- What opportunities exist to improve cooperation and what are the barriers to success?

Panel Topics:

1. Calibrating the Threat
2. China's Approach to Cyber Competition and Cooperation
3. Allied Cooperation: Defining the Baseline
4. Lessons from the Transatlantic Community
5. Implementing Persistent Engagement
6. Strengthening Collective Cyber Defense
7. Strengthening Cyber Diplomacy
8. Framing the Main Strategic Choices

Day 1: Framing the Problem

Panel 1: Calibrating the Threat

- What are the main features of the regional cyber threat?
- Are there significant differences of assessment among allies?

Commonwealth of Australia. *Australia's Cyber Security Strategy 2020*. Department of Home Affairs, 2020. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

> To counter increasingly sophisticated nation-state and criminal cyber threats, Australia's 2020 strategy elevates the role of individuals and companies in defending against malicious actors while planning more robust international cybersecurity partnerships. With the main focus on protecting against state-sponsored actors, the document emphasizes the need to correctly prioritize between offensive and defensive capabilities. Australia must meet the challenges of an evolving cyber threat landscape by simultaneously developing the personnel and creating the offensive weapons necessary to deliver a "proportionate" response in the event of a cyber attack from a nation-state. This report also commits to new initiatives to enhance regional and international partnerships, highlighting the Cyber Cooperation Program in the Indo-Pacific region.

Government of Japan. *Defense of Japan 2020*. Ministry of Defense, 2020. https://www.mod.go.jp/e/publ/w_paper/wp2020/pdf/index.html

> Recognizing the increasing severity of cyber attacks and growing vulnerabilities, the 2020 white paper outlines ongoing and new responses to the threats posed to defense and civilian networks by nation-states and non-state actors. The 2020 assessment points specifically to the diverse and aggressive cyber attacks on information and communication networks by China, Russia, Iran, and North Korea. The emerging security environment necessitates international cooperation and cross-domain collaboration. Japan maintains a cooperative focus that prioritizes threat intelligence sharing, capacity building within Asia, and participating in NATO's multilateral cyber exercises. Domestically, the Government of Japan will undertake a nation-wide campaign to invest in building cyber personnel and the emerging technologies that will automate cyber defensive and offensives capabilities.

Lin, Bonny, Michael Chase, Jonah Blank, Cortez Cooper III, Derek Grossman, Scott W. Harold, Jennifer D.P. Maroney, Lyle J. Morris, Logan Ma, Paul Orner, Alice Shih, and Soo Kim. "Regional Responses to U.S.-China Competition in the Indo-Pacific." Santa Monica, CA: RAND Corporation, RR-4412-AF, 2020. https://www.rand.org/pubs/research_reports/RR4412.html

> This 2020 RAND study examines the opportunities for the United States' cyber cooperation with Indo-Pacific states to contest China's aggressive cyber policy that jeopardizes a free and open Indo-Pacific internet. The report suggests a three-part

solution for the United States, starting first with bolstering Australian, South Korean, and Japanese cyber readiness and capacity to counter Chinese cyber espionage. Second, the authors recommend welcoming India into regional cyber information and training exercises. In addition to the United States' traditional allies, the third step is a partnership with Singapore and Malaysia, identified as the two best Southeast Asian partners to prevent China's campaign to dominate regional internet and 5G architecture that will influence economic development and limit a free and open virtual Indo-Pacific. Overall, the report concludes that the United States' regional policy should stress the economic benefits to cyber cooperation.

Republic of Korea. *National Cybersecurity Strategy*. National Security Office, 2019. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf

The 2019 strategy statement calls for whole of country preparation against cyber attacks on the nation's core infrastructure as well as industrial base while also advocating for international rules in cyber space. As cyber attacks increase, the strategy highlights the need to bolster communication networks, incorporate private sector operators into response efforts, and protect government information from malicious actors. Officially, the Republic of Korea urges stronger bilateral and multilateral agreements that will generate international norms to build trust and prevent escalatory spirals in cyberspace. Through creating a culture of national cyber stability, the strategy aims to protect its citizens and their rights via international cooperation alongside domestic cyber hygiene campaigns.

Rasser, Martijn. "Networked: Techno-Democratic Statecraft for Australia and the Quad." Center for A New American Security, January 19, 2021. https://www.cnas.org/publications/reports/networked-techno-democratic-statecraft-for-australia-and-the-quad

This report urgently calls for a new multilateral commitment to cybersecurity and emerging technology cooperation among members of the Quadrilateral Security Dialogue. The author insists that China's malicious actions in cyberspace require collaboration to safeguard a free and open virtual Indo-Pacific. Feasible lines of cooperative effort include shared threat intelligence, harmonizing law enforcement responses, discussion on norms in cyberspace, and a cyber attack mitigation network to monitor and resolve network intrusions. Although all members of the Quad would play a role in bolstering the alliance's cybersecurity architecture, Australia is poised to lead the Quad's cybersecurity alliance thanks to its years of cooperation that built a regional and global cyber network.

United States of America. *A Free and Open Indo-Pacific Advancing a Shared Vision*. Department of State, November 4, 2019. https://www.state.gov/wp-content/uploads/2019/11/Free-and-Open-Indo-Pacific-4Nov2019.pdf

> The Department of State's vision for the Indo-Pacific prioritizes defending the region's connectivity from attacks by state and non-state actors. Malicious actors use the region's internet architecture to advance interests that jeopardizes Indo-Pacific peace and security. The United States coordinates with allies and partners to ensure network stability by building capacity, creating cyber policy frameworks, and promoting cyber awareness for the region's residents. Digital partnerships between the United States' and Indo-Pacific's private sectors develop local economies by building resilient networks and fostering mutually beneficial economic growth. The United States' interests in the region are preserved by working with Indo-Pacific states to guarantee a stable cyber domain.

Panel 2: China's Approach to Cyber Competition and Cooperation

- How does China perceive the cyber threat environment and what opportunities does it see to bolster its influence?
- What are China's military and political strategies for meeting the cyber threat landscape?
- What is China's agenda for promoting international cooperation to mitigate these threats or capitalize on opportunities?

Buchanan, Ben and Fiona S. Cunningham. "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis." *Texas National Security Review* 3, no. 4 (Fall 2020): 54-81. https://tnsr.org/2020/10/preparing-the-cyber-battlefield-assessing-a-novel-escalation-risk-in-a-sino-american-crisis/

> In the context of rapidly deteriorating Sino-American relations, the authors contend that a political crisis between the two countries could escalate into an armed conflict. Buchanan and Cunningham determine that there is a genuine risk of escalation in a future Sino-American crisis if either country discovers a network intrusion amidst a crisis and uses force in response. Much of this risk is derived from the difficulty in distinguishing cyber espionage from operations to set the battlefield. China's ostensible confusion regarding these risks and opacity behind motivations for both sides' network intrusions amplifies the possibility of escalation. Steps to mitigate the risks of misperception should be focused on increasing Chinese awareness, and perhaps U.S. Cyber Command explaining the risk management principles they employ.

Campbell, Alex. "Persistent Engagement with Chinese Characteristics." *Lawfare*, September 18, 2019. https://www.lawfareblog.com/persistent-engagement-chinese-characteristics

> Writings from the People's Liberation Army's on information warfare demonstrate that China sees cyberspace as a strategically salient vector for achieving political goals below the threshold of armed force. The reactions of Chinese sources to the U.S. strategy of

Defend Forward appear subdued or confused, Campbell argues. They depict it as a stronger, more offensive version of deterrence, instead of a strategy that involves continual preemptive operations against Chinese cyber capabilities. The author concludes it may be necessary for the United States to provide more explicit statements as to the goals of persistent engagement to Chinese leadership. Clarity, not opacity, will best serve the United States' interests and inform senior Chinese leadership of a strategic shift.

International Institute for Strategic Studies. "China's Cyber Power in a New Era." In *Asia Pacific Regional Security Assessment 2019*. May 2019. https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5

China aspires to become not only the world's largest nation in cyberspace but also a cyber superpower. This report assesses the positive and negative attributes of this goal. Cyberspace presents new risks that for the Chinese Communist Party (CCP) that require deft management as well as benefits that are integral to the CCP's future. From an economic perspective, the CCP sees the vibrancy of the digital economy and innovation in emerging technologies as central for driving future development and bolstering regime legitimacy as traditional economic growth slows. However, the internet represents an existential threat to the CCP by creating a new commons for public discussion and dissent. Beijing also views cyber espionage as a potent tool for advancing its economic, political, and strategic aims that can be employed below the threshold for armed conflict.

Jinghua, Lyu. "A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward'." *Lawfare*, October 19, 2018. https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward

In this critique of Defend Forward, Lyu Jinghua argues that this shift is largely unjustified and potentially dangerous. According to Lyu, the more "aggressive" U.S. operational posture—together with significant improvements in U.S. cyber capabilities—will cause nervousness in countries that the United States has listed as security challenges, namely China, and increase the likelihood of unintentional crisis and escalation. From China's perspective the United States already enjoys a significant cyber advantage, and China's intentions in cyberspace promote peace, stem cyber crises, and ensure national network and information security for domestic stability. Lyu recommends that the United States reorient its cyber policy towards self-restraint to avoid feeding a volatile cyber threat environment.

Segal, Adam. "China's Pursuit of Cyberpower." In *The Future of Cybersecurity Across the Asia-Pacific*. *Asia Policy* 15, no. 2 (April 2020): 60-66. https://www.nbr.org/wp-content/uploads/pdfs/publications/ap15-2_cyberrt_apr2020.pdf

According to Segal, China is one of the Indo-Pacific's most active cyber actors, frequently conducting cyber operations to strengthen its economic competitiveness, accelerate the modernization of the People's Liberation Army, weaken opponents of the Chinese

Communist Party (CCP), resist international pressure and foreign ideas, and offset the United States' conventional military dominance. Chinese officials, on the other hand, also see their cybersecurity as weak relative to the degree of threat and the capabilities they perceive from potential adversaries due to two major sources: an underdeveloped cybersecurity regulatory framework, and widespread dependence on foreign technology in critical networks. Even though the potential for Beijing to use destructive cyberattacks in a conflict is high, Chinese leaders are likely aware they are vulnerable to similar attacks.

Panel 3: Allied Cooperation: Defining the Baseline

- To what extent do allied approaches to cybersecurity converge or diverge?
- What lessons stand out from past efforts to strengthen cooperation among allies?

Bartlett, Benjamin. "Japan: An Exclusively Defense-Oriented Cyber Policy." In *The Future of Cybersecurity Across the Asia-Pacific*. *Asia Policy* 15, no. 2 (April 2020): 93-100. https://www.nbr.org/wp-content/uploads/pdfs/publications/ap15-2_cyberrt_apr2020.pdf

This article highlights Japan's uniquely defensive approach to cybersecurity to protect itself from regional adversaries and comply with its "exclusively defense-oriented" national security policy. Japan's dependence on technology is seen in both its technology-based economy and its technologically advanced military. Japan's national security concerns stem from Russian hybrid warfare, Chinese cyberespionage, and North Korean cybertheft. Due to Article 9 of Japan's constitution that limits use of force coupled with a defense spending cap of 1 percent of gross domestic product, Japan has chosen to strategically invest in cybersecurity defensive capabilities focusing on protecting its critical and digital infrastructure.

Ebert, Hans and Laura Groenendaal. "Cyber Resilience and Diplomacy in the Republic of Korea." *Digital Dialogue*, August 18, 2020. https://eucyberdirect.eu/content_research/cyber-resilience-and-diplomacy-in-the-republic-of-korea/

South Korea's reactive national cybersecurity strategy stems from North Korean intrusions and a worsening cyber threat environment in the Indo-Pacific. South Korea remains vulnerable to cyber attacks despite possessing a sophisticated cyber weapons arsenal and an economy reliant on information technologies. The country's strategy is centered on ensuring the resilience of critical infrastructure alongside public-private information networks. South Korean policy makers identified cybersecurity pipeline issues to encourage university-level programs for ethical hackers. The European Union's close ties to South Korea indicate potential diplomatic opportunities to enforce global norms and fight cyber crime in conjunction with allies.

Harold, Scott W., Derek Grossman, Brian Harding, Jeffrey W. Hornung, Gregory Poling, Jeffrey Smith, Meagan L. Smith. "The Thickening Web of Asian Security Cooperation: Deepening Defense Ties Among U.S. Allies and Partners in the Indo-Pacific." Santa Monica, CA: RAND Corporation, RR-3125-MCF, 2019. https://www.rand.org/pubs/research_reports/RR3125.html

> This RAND report highlights the benefits for the United States' security when allies such as Japan, South Korea, and Australia create strong cyber partnerships with non-U.S. treaty allies such as India, Indonesia, and Vietnam. These partnerships build regional cyber norms and capacity, ultimately aiming for increased cyber stability to prevent cyber espionage and crime. The authors note that even the most technologically advanced countries in the region have cybersecurity gaps and suggests the United States could step in to create a shared database of cyber threats and communicate best practices for the Indo-Pacific. This would help resolve discrete national cybersecurity concerns while encouraging further regional cooperation that is aligned with U.S. goals—including the incorporation of India into Indo-Pacific cybersecurity architecture.

Runde, Daniel F., Conor M. Savoy, and Owen Murphy. "Post-Pandemic Infrastructure and Digital Connectivity in the Indo-Pacific." Center for Strategic and International Studies, November 2, 2020. https://www.csis.org/analysis/post-pandemic-infrastructure-and-digital-connectivity-indo-pacific

> This piece argues that infrastructure development in the Indo-Pacific can be an avenue for further cooperation among U.S. allies as governments in the region seek to diversify both physical and digital infrastructure funding. Covid 19 has exacerbated infrastructure issues in the Indo-Pacific, highlighting the need for a digital economy to ensure pandemic relief and to allow for continued economic activity. The authors stress that the Indo-Pacific is a "digital frontier" with cooperation opportunities in building cybersecurity legal frameworks, technological literary, e-commerce, internet access, and allied foreign investment. The authors recommend countries invest in broadband infrastructure, USAID identified infrastructure needs, and for the United States to open a Strategic Investment Fund for Indo-Pacific digital infrastructure.

Williams, Brandon Kirk. "An Opportunity for Strengthening U.S.-Australian Cyber Cooperation." *Lawfare*, September 16, 2020. https://www.lawfareblog.com/opportunity-strengthening-us-australian-cyber-cooperation

> Australia recently made its largest-ever investment in cybersecurity in 2020 to address a tide of Chinese-linked cyberattacks against Australia. Williams suggests that this is an opportunity to strengthen U.S.-Australian cooperation within the Indo-Pacific after mixed signals from Washington put the United States' commitment to Indo-Pacific security in question. Given Australia's reinvestment in cybersecurity coupled with a new cybersecurity strategic doctrine, the author highlights three areas for U.S.-Australian cooperation: 1) resumption of a U.S.-Australian Track 1.5 cybersecurity dialogue, 2) increased cooperation between the Australian Cyber Security Centre and U.S. Cyber Command, and 3) continued investments from Washington in Australia's cybersecurity technology and academic sectors.

Day 2: Learning Lessons

Panel 4: Lessons from the Transatlantic Community

- How have the United States and its European allies approached cooperation for cyber security?
- What are the different roles of NATO and the European Union?
- Are there lessons relevant to the further strengthening of allied cooperation in the Indo-Pacific?

Frühling, Stephan. "'Key to the Defense of the Free World': The Past, Present and Future Relevance of NATO for US Allies in the Asia–Pacific." *Journal of Transatlantic Studies* 17 (2019): 238–54. https://doi.org/10.1057/s42738-019-00014-0

> Frühling asserts that NATO can serve as a strategic partner to Indo-Pacific countries and should be utilized as a platform for cyber cooperation between the Indo-Pacific and Euro-Atlantic regions. The author argues that NATO can apply lessons from deterring Russia through the use of interoperable partnerships when it collaborates with Indo-Pacific states. NATO can also leverage these partnerships to better operationalize joint exercises. Cybersecurity, due to its borderless nature, is a rich area for NATO to launch strategic partnerships. NATO's experience with hybrid warfare positions it to export its strategies to the Indo-Pacific to deter regional aggression across domains.

Kramer, Franklin D., Lauren Speranza, and Conor Rodihan. "NATO Needs Continuous Responses in Cyberspace." *New Atlanticist*, December 9, 2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/

> This piece argues that NATO's approach to cyber threats, particularly from Russia and China, has been reactive and disjointed. This article proposes that NATO utilize its charter to require better individual national cybersecurity defensive practices while leveraging collective knowledge to build capacity across NATO member states. The authors recommend NATO require members to implement resilient cyber architecture and critical infrastructure, establish Standing Cybersecurity Hunt Teams in coordination with the NATO Cooperative Cyber Defence Centre of Excellence, and coordinate persistent engagement strategies in coordination with NATO's Cyberspace Operations Centre.

Renard, Thomas. "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain." *European Politics and Society* 19, no. 3 (2018): 321–37. https://doi.org/10.1080/23745118.2018.1430720

> Renard notes that the European Union (EU) has developed a number of strategic, bi-lateral cybersecurity partnerships with allied cyber powers, adversarial cyber powers, and less developed countries. This type of varied cyber diplomacy positions the EU as an agile global cybersecurity interlocutor and norms builder. The EU maintains critical partnerships with NATO and the United States alongside secondary partnerships with

adversaries to preserve open lines of communication and situate itself favorably to influence developing regions. The United States can mirror the EU's wide ranging cyber diplomacy in the Indo-Pacific by prioritizing issues such as cyber crime that afflicts every state in the region.

Schuetze, Julia. "The Future for EU-US Cybersecurity Cooperation." *Directions Blog*, November 26, 2020. https://directionsblog.eu/the-future-for-eu-us-cybersecurity-cooperation/

Schuetze contends that the United States and the European Union (EU) have two foundational shared views of cyberspace: cybersecurity is a national security interest, and foreign and security policy tools can strengthen cybersecurity. They diverge, however, on the methodology of responding to malicious cyber activities. The United States employs a doctrine of Defend Forward of offensive cyber operations, and the EU relies on the diplomacy-oriented Cyber Diplomacy Toolbox. Despite these differences, the United State and the EU can act as a model for cyber diplomatic cooperation by focusing on common ground such as cyber crime, conducting joint cyber exercises, and exchanging cyber liaisons to share best cyber diplomacy practices.

Smeets, Max. "U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection." *Intelligence and National Security* 35, no. 3 (2020): 444–53. https://doi.org/10.1080/02684527.2020.1729316

Smeets argues that increased U.S. Cyber Command operations within allies' networks without consent could create friction and mistrust. Defend Forward may trigger unexpected consequences such as a loss of allies' intelligence gathering or adversaries' manipulation of allies' distrust once network exploits are uncovered. Cyber Command's persistent engagement may be best suited for allies that lack the cyber capabilities to defend their own networks. This could open new doors for cooperation with countries that have limited cyber capacity in the Indo-Pacific. It also highlights the need for bilateral talks and the development of memorandums of understanding with current and future allies to ensure alliances operate smoothly.

Panel 5: Implementing Persistent Engagement

- How much progress has been made in developing and implementing joint doctrine?
- How much progress has been made in developing the needed coordination between CYBERCOM and INDOPACOM? With allies?
- What more should and can be done?

Fischerkeller, Michael P. "Opportunity Seldom Knocks Twice. Influencing China's Trajectory via Defend Forward and Persistent Engagement in Cyberspace." *Asia Policy* 15, no. 4 (October 2020): 65-89.
https://www.nbr.org/publication/opportunity-seldom-knocks-twice-influencing-chinas-trajectory-via-defend-forward-and-persistent-engagement-in-cyberspace/

Fischerkeller argues that denying China the ability to conduct intellectual property (IP) theft and fueling its economic growth from pilfered technology must be one of the United States' primary cyber missions. He contends that China's economy is slowing due to a lack of indigenous innovation. If the United States wishes to reduce competition by impeding further IP theft, Defend Forward is an ideal policy solution. China launched its five-year plans at a time when Cyber Command was still in its infancy. Now, as a functioning command, it can simultaneously harden domestic networks while actively disrupting malicious actions in cyberspace. The author justifies why the United States is well within its right to devise a policy to resist further theft by pointing to Xi Jinping's failed promise to President Obama to cease IP theft as evidence that a bold strategy is necessary.

Platte, James E. "Defending Forward on the Korean Peninsula: Cyber Deterrence in the U.S.-ROK Alliance." *The Cyber Defense Review* 5, no. 1 (Spring 2020): 75-92. https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2006_Platte_WEB.pdf

Although the U.S.-ROK alliance is predicated on extended deterrence, less clarity exists for the United States' cyberspace commitments occurring in the gray zone. Platte argues any North Korean attack below the threshold of armed conflict or that can include escalating strategic effects must be defended against. The United States, Platte argues, maintains significant security interests in South Korea's cyber stability and should implement persistent engagement in partnership with South Korea. Both countries should codify this partnership in a joint cyberspace deterrence doctrine and create an allied cybersecurity unit designed to deter North Korea, simultaneously demonstrating the United States' overwhelming commitment to the alliance while showcasing the alliance's asymmetric advantage.

Rovner, Joshua. "More Aggressive and Less Ambitious: Cyber Command's Evolving Approach." *War on the Rocks*, September 14, 2020. https://warontherocks.com/2020/09/more-aggressive-and-less-ambitious-cyber-commands-evolving-approach/

Rovner argues that after implementing Defend Forward, Cyber Command adopted a more aggressive approach towards combating adversaries, one centered on diminishing Red's chances of success while acknowledging the limits of deterrence and coercion in cyberspace. Cyber Command must continue engaging in a risk assessment process to guarantee it does not antagonize allies while simultaneously upholding agreed upon norms. Cyber Command's goal to ensure joint, collective security through collaboration and preemption must prioritize threat intelligence sharing and avoid the temptation to collect on friendly networks. Furthermore, Cyber Command should be willing to forego important operations at the request of allies if concerns about the mission exist, demonstrating the United States' commitment to partnership.

Smeets, Max. "Cyber Command's Strategy Risks Friction with Allies." *Lawfare*, May 28, 2019. https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies

> While Cyber Command's Defend Forward strategy via global engagement sounds promising, policymakers have must define what this cyber doctrine means for alliances and partnerships. Cyber Command aims to actively disrupt and directly counter adversaries even if this requires a presence in allied countries' networks. Given cyber's nature, this may mean launching impromptu attacks or operations without prior notice and agreement from the host country. Failing to secure this approval before acting will likely undermine allied confidence and trust. Adversaries like Russia will then be poised to exploit these fissures and deliberately route their activity through allied cyberspace, spurring further United States activity and eroding level of trusts. Policymakers must take allies' political calculus into consideration while implementing Defend Forward.

White, Timothy J. "Joint Operations in Cyberspace: From Operational Unity to Shared Strategic Culture." In "Ten Years In: Implementing Strategic Approaches to Cyberspace." Newport Papers, Newport, RI: U.S. Naval War College, 2020: 129-140. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers

> White highlights the inherently shared nature of cyberspace and calls for the United States to embrace all dimensions, both civilian and military, as a platform for projecting power. Permeating all traditional domain borders, cyber requires constant engagement and singular, unified operations as opposed to piecemeal joint efforts. While the Cyber National Mission Force (CNMF) has already embraced these new concepts and stresses reliance upon international partnerships, it is hindered by bureaucratic battles within the Department of Defense and therefore struggles to cultivate the cyber entity necessary to present a robust defense with allies. CNMF's long-term success hinges upon an understanding of joint functionality, reliance upon both defensive and offensive tactics, and a restructuring of cyber equities in the Department of Defense.

Day 3: Next Steps

Panel 6: Strengthening Collective Cyber Defense

- What should and can be done to enhance cooperation among the United States and its allies?
- Are new institutions needed? To do what?
- Is a special form of leadership required? If so, who can provide it?

Demchak, Chris G. "Cyber Competition to Cybered Conflict." In "Ten Years In: Implementing Strategic Approaches to Cyberspace." Newport Papers, Newport, RI: U.S. Naval War College, 2020: 47-66.

https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1044&context=usnwc-newport-papers

> To counter China's authoritarian and increasingly antagonistic actions in cyberspace, the United States and its partners must view the internet as a defense-oriented domain dependent on governance structures instead of a free marketplace of ideas. Demchak recommends that the United States and allies create a cyber operational resilience alliance to subvert Chinese influence while restructuring national systems to foster a secure, cooperative security environment. China is mobilizing its instruments of national power in cyberspace while the United States' public and private leaders have failed to remedy systemic vulnerabilities. Additional partnerships with the telecommunications and information technology industries are necessary to build cyber defense measures and raise awareness of Chinese activity.

Heinl, Caitríona. "Navigating Cyber Diplomacy in the Asia Pacific." *Directions*, November 1, 2020. https://directionsblog.eu/navigating-cyber-diplomacy-in-the-asia-pacific/

> As cyber and digital competition in the Indo-Pacific accelerates, Australia has embarked on a mission to encourage norms on responsible state behavior in cyberspace and build cyber capacity with regional partners. Heinl reports that cyber ambassadors such as Australia's Tobias Feakin insist that countries must embrace cyber's expanding centrality for diplomacy to share best practices and reinforce efforts at the United Nations to craft binding laws and norms. Australia's Cyber Cooperation Program invests in cyber resilience and capacity building efforts within the Indo-Pacific to prevent cybercrime, protect human rights, and enforce the rule of law among states in cyberspace.

Lee, Kristine, Joshua Fitt, and Coby Goldberg. "Renew, Elevate, Modernize: A Blueprint for a 21st-Century U.S.-ROK Alliance Strategy." Center for New American Security, November 16, 2020. https://www.cnas.org/publications/reports/renew-elevate-modernize-a-blueprint-for-a-21st-century-u-s-rok-alliance-strategy

> To adequately prepare the U.S.-ROK alliance for the twenty-first century, both countries must commit to advancing cooperation on new policy areas ranging from cyber to emerging technologies. Possible actions include partnering the Defense Innovation Unit with Microsoft's Cybersecurity Center to identify threats, organizing a Department of Commerce cyber trade mission, and coordinating U.S.-ROK digital strategies to embrace capacity building. The United States should also look to improve the ROK-Japan relationship through a focus on shared cybersecurity challenges, creating a larger network of defense cooperation and alliances in the Indo-Pacific.

Lee, Sang, Ainsley Katz, Karrie Jefferson, Val Cofield, and Laura Bate. "The Cyberspace Solarium Commission on Norms." *Council on Foreign Relations - Net Politics*, April 16, 2020. https://www.cfr.org/blog/cyberspace-solarium-commission-norms

> The authors summarize a key finding from the Cyberspace Solarium Commission that there is a widespread failure to adhere to international cyber agreements and acceptable

practices. The United States must utilize its diplomatic tools to encourage the enforcement of treaties and conventions as well as promoting the establishment of an international coalition dedicated to setting norms in cyberspace. These collaborative and capacity-building measures will ultimately enable a layered cyber deterrence strategy and stronger attribution abilities for the United States and its allies. These actions are wholly dependent on non-military power and cyber diplomacy, and the Department of State's Bureau of Cyberspace and Emerging Technologies should lead these cooperative efforts.

Reiber, Jonathan and Benjamin Bahney. "The U.S. Government Can Deepen Its Operational Partnership With the Private Sector to Better Defend the U.S. in Cyberspace." *Lawfare*, March 13, 2020. https://www.lawfareblog.com/us-government-can-deepen-its-operational-partnership-private-sector-better-defend-us-cyberspace

To enhance the effectiveness of Defend Forward, Reiber and Bahney argue that the U.S. government must increase its collaboration with the private sector. While the government is ultimately responsible for defending the country, the bulk of cyberspace is operated by the private sector and should be called upon to help reduce risk and deescalate crises in possible conflicts. The authors urge federal and private entities to utilize scenario planning to establish frameworks to protect networks and share perspectives on each sectors' primary responsibilities. Joint public-private cyber discussions routed through government institutions, such as the Enduring Security Framework, provide venues for trust building, joint operations, and threat intelligence sharing that will harmonize public and private efforts to protect the United States.

Panel 7: Strengthening Cyber Diplomacy

- What are the roles of diplomacy in supporting cyber security?
- How can diplomatic strategies balance cyber competition and cyber security cooperation?

Barrinha, Andre and Thomas Renard. "The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace." *Council on Foreign Relations - Net Politics*, June 10, 2020. https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace

The authors chronicle cyberspace's evolution into a post-liberal domain where the power relations, values, and institutions that governed it are challenged by states absent from its genesis. Worrying evidence of change includes the Chinese proposals to replace the backbone of the internet and myriad countries' support for Russia's proposed international cybercrime treaty. A post-liberal trend has also seen the increasing politicization and weaponization of cyberspace that catalyzed the emergence of cyber diplomacy. As more countries acquire offensive cyber capabilities, cyber diplomacy is sorely needed to prevent escalation, facilitate dialogue, develop norms of responsible

state behavior, and to bridge conflicting visions of what the institutions governing cyberspace should resemble.

Chernenko, Elena, Oleg Demidov, and Fyodor Lukyanov. "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." Council on Foreign Relations, February 23, 2018. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

Information and communications technology presents one of the most critical modern challenges to global security, and there is an urgent need for cooperation among states to mitigate threats such as cybercrime, cyberattacks on critical infrastructure, or electronic espionage. Contrary to common perception, the authors illustrate, most cyber threats materialize as diverse, complex threats to the increasingly digitalized global economy, rather than massive, state-sponsored attacks on critical infrastructure. A whole of society approach including governments, global industry, academia, and civil society is needed to tackle such a widespread and complex threat. These actors should cooperate in governance forums to enforce accepted norms in cyberspace, with an eye to building future institutions that reign in cyber threat actors.

Goldman, Emily O. "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy." *Texas National Security Review* 3, no. 4 (Fall 2020): 84-101. https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/

Goldman writes that the traditional approach of cyber diplomacy to establish responsible norms of state behavior in cyberspace has largely foundered, in part due to the failure of critical states such as China and Russia to abide by norms sought by the United States. The author recommends that the Department of State should reexamine its assumptions about cyber conflict and norm emergence and develop competitive, Defend Forward policies focused on seizing the initiative from adversaries whose cyberspace campaigns erode the United States' national security. Cyber leadership from the Department of State can increase the speed, agility, and scale of Defend Forward by building coalitions while reorienting perspectives on cyber conflict.

Mazanec, Brian M. and Nick Marinos. "State Has Not Involved Relevant Federal Agencies in the Development of its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau." U.S. Government Accountability Office, September 22, 2020. https://www.gao.gov/assets/710/709563.pdf

In 2019, the Department of State notified Congress of its intent to establish a new Cyberspace and Emerging Technologies Bureau (CSET) to align cybersecurity and emerging technologies issues with the department's national security efforts. CSET aimed to improve coordination with other agencies working on national security issues and promote long-term technical capacity within the Department of State. This report finds that the Department of State has not engaged with other agencies to prevent fragmentation, overlap, and duplication of efforts. Although CSET will boost the United

States' cyber diplomacy, it must first coordinate within government to ensure effective implementation of its agenda.

Painter, Chris. *"*Diplomacy in Cyberspace*." The Foreign Service Journal* 95, no. 5 (June 2018): 26-30. https://www.afsa.org/diplomacy-cyberspace

Painter argues that the dramatic uptick in the number and sophistication of technical threats in cyberspace, as well as serious policy threats driven by repressive regimes, places the nature and governance of the internet as we know it at risk. Managing these issues will require an unprecedented application of cyber diplomacy by the United States. Events of the past few years have shown that properly applied, cyber diplomacy has the potential to advance the United States' agenda of an open and secure internet where robust cyber defense can convinced advanced persistent threats to abandon intellectual property theft or employ cyber espionage to threaten the United States' core values.

Panel 8: Framing the Main Strategic Choices

- What lessons can be drawn from the workshop's discussion about how to strengthen allied cybersecurity cooperation?

Center for Global Security Research, Lawrence Livermore National Laboratory. "Strategic Competition in Cyberspace: Challenges and Implications. Workshop Summary." Livermore, CA: CGSR, 2019.
https://cgsr.llnl.gov/content/assets/docs/CGSRCyberWorkshop2019SummaryReport.pdf

This 2019 workshop summary emphasizes the central role allies can play in cybersecurity, yet the summary acknowledges difficulties facing cyber cooperation. Allies such as Japan lead in technology development or, in the case of Australia, shape regional 5G architecture by opposing Huawei. Participants recommended cyber exercises to boost interoperability outside of the Five Eyes intelligence alliance. Cyber cooperation, however, struggles to transcend national defense, commercial, and intelligence priorities. Setting norms on expectations and technological baselines establishes a foundation for Indo-Pacific cooperation to overcome differences.

Center for Global Security Research, Lawrence Livermore National Laboratory. "Cyberspace, Information Strategy, and International Security. Workshop Summary." Livermore, CA: CGSR, 2018.
https://cgsr.llnl.gov/content/assets/docs/CGSR_Cyber_Workshop_2018_Summary_Report_Final2.pdf

CGSR's 2018 workshop summary noted the progress and limits for the United States' Indo-Pacific allies. Australia cemented its place in the regional order by building national cyber institutions to protect against cyber criminals and cyber espionage, hoping at the

time to prevent Chinese cyber coercion. Japan, on the hand, faced constitutional limits on developing offensive cyber capabilities. Both Japan and Australia viewed norm setting as a principal goal to prevent failure of the region's cyber stability. The report noted, overall, progress was not yet achieved in building cyber defensive capacity to protect against advanced persistent threat actors.

Center for Global Security Research
Lawrence Livermore National Laboratory
P.O. Box 808, L-189 Livermore, California 94551
https://CGSR.llnl.gov

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory
under Contract DE-AC52-07NA27344. LLNL-TR-819993